DELL Technologies

Présentation de la solution

Personnalisation de Secure Boot UEFI de Dell EMC PowerEdge

Les environnements de serveur de datacenter concentrent traditionnellement une grande partie de leurs efforts de sécurité au niveau du système d'exploitation, des applications et du réseau. À mesure que les préoccupations en matière de sécurité de l'infrastructure matérielle augmentent, la complexité augmente pour les administrateurs de la sécurité IT. L'un des besoins fondamentaux des équipes IT responsables des serveurs et de la sécurité consiste à mettre en place une base informatique de confiance et à étendre cette confiance aux systèmes d'exploitation et aux applications. Généralement réservée aux applications et aux jeux de données les plus sécurisés et les plus sensibles, la sécurité de l'infrastructure personnalisée prend rapidement de l'importance. L'évolution de la menace qui pèse sur le matériel des serveurs exige une approche plus complète, notamment la personnalisation de Secure Boot UEFI, pour renforcer cette base de confiance.

Cela commence par l'architecture cyber résiliente Dell EMC, qui valide le BIOS et le firmware d'iDRAC (Integrated Dell Remote Access Controller) avant son chargement. Le firmware pour d'autres composants critiques est également validé à l'aide de certificats de chiffrement stockés afin de garantir que le firmware authentique est exécuté sur le serveur.

Architecture cyber-résiliente Dell EMC

Protection efficace

- Racine de confiance matérielle au niveau de la puce
- Mises à jour de firmware signées
- System Lockdown
- Sécurisation du mot de passe par défaut

Détection fiable

- Détection de dérive de la configuration et du firmware
- Journalisation des événements persistant, y compris l'activité utilisateur
- Alertes sécurisées

Récupération rapide

- Récupération automatique du BIOS
- Restauration rapide de l'OS
- System Erase

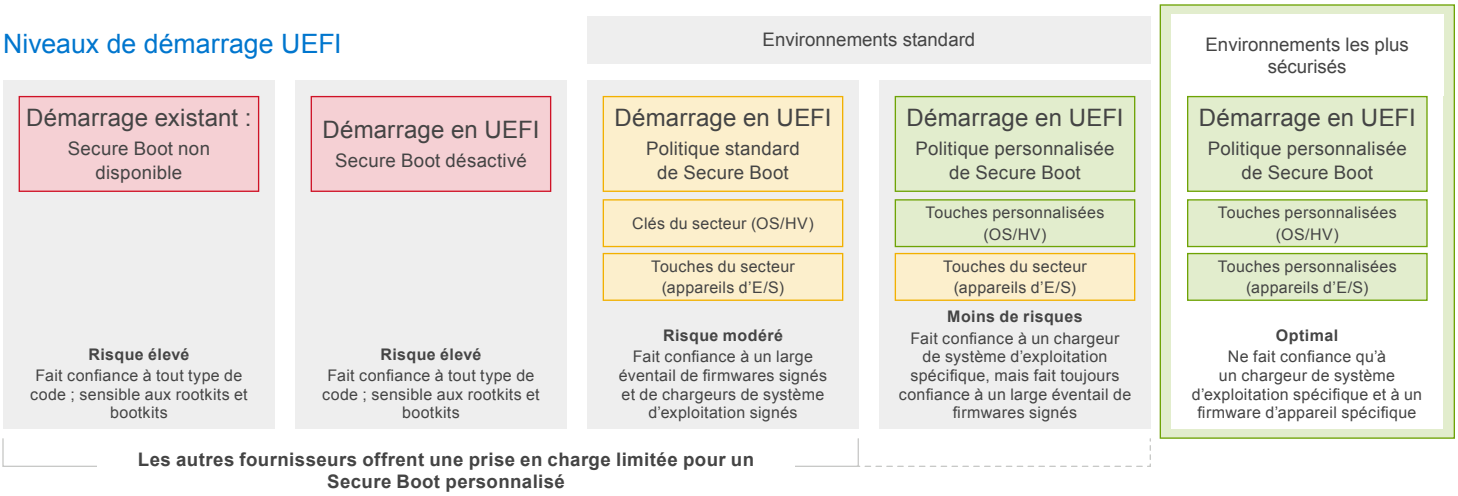
En tant que remplacement moderne des contrôles de configuration et de démarrage du BIOS existants, Secure Boot UEFI initialise les fonctions de base du serveur avant le démarrage d'un hyperviseur ou d'un système d'exploitation. Les serveurs PowerEdge utilisent Secure Boot UEFI pour vérifier les certificats générés par chiffrement des pilotes UEFI et les chargeurs de démarrage du système d'exploitation. Il s'agit des « clés » qui permettent au serveur de valider les éléments suivants :

- Pilotes UEFI chargés à partir de cartes PCIe,
- Pilotes UEFI et exécutables chargés à partir d'appareils de stockage de masse,
- Chargeurs de démarrage du système d'exploitation : généralement Linux ou Microsoft Windows.

Ce processus de validation est essentiel à la protection du serveur contre l'initiation non autorisée du code avant le lancement du système d'exploitation. En vérifiant la signature du chargeur de démarrage, du noyau et d'autres codes d'espaces utilisateurs, la validation du firmware UEFI est conçue pour interdire l'exécution des logiciels non signés sur le système.

La personnalisation de Secure Boot UEFI de Dell EMC PowerEdge offre également la possibilité unique de prendre en charge les certificats personnalisés générés et signés par une autorité autre que Microsoft. Microsoft est l'autorité de certification par défaut pour les appareils et systèmes d'exploitation pris en charge par UEFI. De nombreuses distributions Linux standard ont mis en œuvre un certificat Microsoft. Dans les situations où un environnement Linux non standard est utilisé (c'est-à-dire des modifications propriétaires du noyau ou des pilotes), il est nécessaire de générer des certificats personnalisés, signés par chiffrement par l'utilisateur, afin d'auto-valider le chargeur de démarrage et de maintenir la chaîne de confiance entre le matériel et le logiciel.

Niveaux de démarrage UEFI



Amélioration de la sécurité des serveurs sans compromis

Le processus de démarrage constitue la base de la sécurité de n'importe quel appareil. Il s'appuie sur une multitude de firmwares qui contrôlent la façon dont les composants et les périphériques d'un appareil sont initiés, ainsi que le chargement du système d'exploitation. Le code antérieur est chargé, plus il est privilégié et plus il peut être endommagé s'il n'est pas authentifié en premier. Si le processus de démarrage est compromis, les pirates peuvent renverser les contrôles de sécurité, ce qui permet d'obtenir un accès non autorisé à diverses parties du système. Il est même possible de créer des ransomwares à l'aide du chargeur de démarrage UEFI malveillants pour prendre le contrôle des serveurs lors du démarrage, reconfigurer l'ordinateur, chiffrer les données et causer des dégâts.

Réduire les risques

Avec des options de configuration et de contrôle modernes, vous êtes mieux équipé que jamais pour protéger vos serveurs contre les attaques de firmwares ou de chargeurs de démarrage. La personnalisation de Secure Boot UEFI de Dell EMC PowerEdge renforce la sécurité de votre infrastructure de serveur tout en laissant de côté les méthodes de démarrage du BIOS existantes. Un avis récent de l'Agence nationale de la sécurité (NSA) du gouvernement américain traite de la question de l'augmentation de la sécurité matérielle des serveurs, citant notamment l'utilisation de la personnalisation de Secure Boot UEFI de PowerEdge comme une méthode qui offre un niveau de sécurité nettement supérieur et la flexibilité nécessaire pour prendre en charge plusieurs systèmes d'exploitation. Dans un rapport technique connexe de la NSA sur la cybersécurité, il est noté que le « mode personnalisé permet au propriétaire du système de restreindre ou d'étendre la sélection de solutions matérielles et logicielles de confiance... » et illustre comment cela peut être réalisé à l'aide de l'utilitaire de configuration UEFI intégré de Dell[1]. Ce contrôle granulaire permet de réduire ou d'éliminer les menaces de mauvaise configuration, d'altération et de logiciels malveillants. Les administrateurs système peuvent réagir plus rapidement aux nouvelles menaces de démarrage et sont protégés contre les éventuelles erreurs de signature de certificats commises par les fournisseurs.

Fonctionnalités de Secure Boot UEFI avec certificats personnalisés

Caractéristiques	Description	Avantages
Secure Boot	• Validation des composants clés et des firmwares.	• Adoption d'une validation de firmware moderne, en laissant derrière les limitations et les menaces de sécurité du BIOS existant.
Certificats auto-signés	• Assurer la sécurité du firmware, du chargeur de démarrage et du lancement du système d'exploitation sur l'ensemble des opérations du serveur.	• Prise en charge des versions de systèmes d'exploitation personnalisés dans le cadre de déploiements hautement sécurisés. • Indépendance par rapport à l'autorité de signature par défaut lors de la mise en œuvre du matériel personnalisé et du firmware associé.
Conformité aux recommandations en matière de sécurité	• Aligné sur les normes de sécurité pour le processus de démarrage des serveurs, la validation des firmwares et la gestion personnalisée des certificats.	• Définit la norme en matière de sécurité du matériel et du firmware du serveur • Positionne les opérations de serveur pour qu'elles soient conformes aux futures recommandations en matière de sécurité des serveurs dans les environnements sensibles.
Intégration avec iDRAC et TPM.	• Tirer parti des fonctions de sécurité existantes du matériel et des firmwares déjà intégrées à la aux serveurs PowerEdge.	• Optimiser la valeur des fonctions de sécurité intégrées pour mettre en place une racine de confiance matérielle complète.

[1] Comme pour la plupart des paramètres système, un administrateur peut utiliser d'autres outils que le programme de configuration du système pour activer la politique standard de Secure Boot. Les outils Deployment Toolkit™ (DTK), Lifecycle Controller™, OpenManage™, la console RACADM et les consoles WS-MAN peuvent également activer la politique standard de Secure Boot.

En savoir plus sur les serveurs PowerEdge

En savoir plus sur Dell EMC OpenManage Enterprise

En savoir plus sur nos solutions de gestion des systèmes

Effectuer une recherche dans notre bibliothèque de ressources

Suivre les serveurs PowerEdge sur Twitter

Contacter un expert Dell Technologies pour une question sur les ventes ou le support

DELL Technologies